چاپ دوم

چگونه با تهدیدات اینترنتی مقابله کنیم

راهنمای آموزشی ویژه دگرباشان جنسی در ایران

این راهنما، خلاصه‌ای است از جزوه «چگونه با تهدیدات اینترنتی مقابله کنیم» که کمیسیون بین‌المللی حقوق بشر زنان و مردان همجنس‌گرا (ایگل‌هِرک) آن را منتشر کرده است. آن‌چه در این‌جا می‌خوانید، تنها خلاصه‌ای است از متن اصلی این جزوه. توصیه می‌کنیم برای مطالعه متن کامل و آگاهی از جزئیات بیشتر، جزوه را از لینک زیر دریافت کنید: http://iglhrc.org/iran/fa/Fa_Publications_Internet_Security

توجه به امنیت در استفاده از کامپیوتر

نخستین گام برای تامین امنیت، نصب یک سیستم عامل مطمئن بر روی کامپیوتر است. از خرید سیستم عامل‌های موجود در بازار که قفل شکسته و ارزان‌قیمت هستند، اجتناب کنید چرا که ممکن است به صورت عمدی یا غیر عمدی دارای مشکلات امنیتی باشند. در صورت امکان، سعی کنید نرم‌افزارهای مورد نیاز خود را از وب‌سایت‌های غیر ایرانی یا از افراد مورد اعتماد و خبره در زمینه کامپیوتر بگیرید.

بسیاری از برنامه‌هایی که به صورت قفل‌شکسته مورد استفاده قرار می‌گیرند، آلوده به بدافزار هستند. تا جایی که امکان دارد، این نرم‌افزارها را بر روی کامپیوتری که ایمنی‌اش برای شما مهم است، نصب نکنید و از نرم‌افزارهای اصل یا رایگانی استفاده کنید که قابل دانلود از سایت اصلی هستند.

سعی کنید برای انتقال اطلاعات کمتر از حافظه‌های خارجی قابل حمل استفاده کنید؛ در صورت امکان، بهتر است کامپیوتری را که بر روی آن اطلاعات حساس دارید به صورت مجزا و ایزوله نگه دارید و برای تفریحات و کارهای روزمره، از یک کامپیوتر دیگر استفاده کنید. یک ضد ویروس مطمئن و کارآمد بر روی کامپیوتر خود نصب کنید. برای امنیت بیشتر، می‌توانید از برنامه‌های «فایروال» که برقراری تماس‌های مشکوک با کامپیوترتان را به شما خبر می‌دهد، استفاده کنید.

استفاده از Microsoft Security Essentials

استفاده از این ابزار امنیت سیستم عامل ویندوز را مطمئن‌تر می‌سازد. اگر ویندوز شما نسخه اصل و قانونی نباشد، می‌تواند شما را دچار مشکلات جدی کند و موجب از میان رفتن تمام امکانات امنیتی ویندوز و حتی از کار افتادن کل سیستم عامل شود. با مراجعه به پیوند زیر می‌توانید یک نرم‌افزار مجانی برای امنیت بیشتر به سیستم عامل ویندوز اضافه کنید:

http://windows.microsoft.com/en-US/windows/security-essentials-download

نگه‌داری از اطلاعات و فایل‌های مهم

اطلاعات شما پس از ذخیره بر روی CD و DVD نمی‌تواند پاک یا آلوده به ویروس شود؛ ولی اگر اطلاعات شما قبل از ذخیره به ویروس یا بدافزار آلوده شده باشد، این بدافزارها روی CD و DVD برای همیشه باقی می‌ماند. ذخیره اطلاعات روی حافظه‌های خارجی و قابل‌حمل، امکان مخفی نگه داشتن یا انهدام فوری اطلاعات را برای شما فراهم می‌کند.

فایل‌ها و اطلاعات شما پاک نمی‌شود

هنگامی که شما یک فایل را از روی کامپیوتر خود پاک می‌کنید و Recycle Bin را هم خالی می‌کنید، هنوز امکان بازیابی آن فایل وجود خواهد داشت. برای جلوگیری از بازیابی اطلاعات پاک شده، می‌توانید از نرم‌افزارهایی مثل «File Shredder» یا «Eraser» استفاده کنید. با این حال، این نرم‌افزارها هم نمی‌توانند از بین رفتن فایل‌ها را به طور کامل تضمین کنند. اگر نگرانی جدی دارید، حافظه کامپیوتر را کاملاً تخریب کنید یا از افراد معتمد متخصص در این زمینه کمک بگیرید.

استفاده از حساب کاربری مخصوص به خود در ویندوز

بهتر است یک حساب کاربری مخصوص خودتان را روی سیستم عامل داشته باشید؛ به‌ویژه اگر افراد دیگری هم از کامپیوتر شما استفاده می‌کنند. حتی برای استفاده‌های مختلف خود هم می‌توانید حساب‌های جداگانه درست کنید.

خطر استفاده از تلفن همراه هوشمند و وسایل تصویر و صدابرداری

استفاده از تلفن همراه برای دسترسی به سرویس‌هایی که شامل اطلاعات مهم هستند و جنبه امنیتی برای شما دارند و یا اگر نگرانی امنیتی خاصی از سوی عوامل حکومتی دارید، توصیه نمی‌شود. در صورتی که تلفن همراه شما دزدیده یا گم شد، گذرواژه تمام سرویس‌هایی را که از طریق آن تلفن از آن‌ها استفاده می‌کردید، تغییر دهید. توجه داشته باشید که سرویس‌های GPS (مکان‌یاب) نصب شده روی این تلفن‌ها می‌تواند موقعیت شما را لو بدهد.

همان‌طور که پیش‌تر در مورد سایر کامپیوترها توضیح داده شد، ممکن است اطلاعاتی که روی حافظه این تلفن‌ها دارید هنوز هم قابل بازیابی باشد. اگر فرد متخصصی در این زمینه نیستید، برای اطمینان از پاک شدن کامل اطلاعات، تنها چاره احتمالا تخریب کامل حافظه یا دستگاه است یا کمک گرفتن از فردی متخصص. اگر امکان تخریب برای شما وجود ندارد، پس از پاک کردن حافظه سعی کنید تمام ظرفیت حافظه را با فایل‌های غیر مهم پر کنید.

امنیت در استفاده از اینترنت

IP یک شناسه اینترنتی است که به هر کاربر در اینترنت تعلق می‌گیرد. هنگامی که در اینترنت به یک آدرس مراجعه می‌کنید، IP شما به آن آدرس متصل می‌شود. با دسترسی به سرویس‌های مختلف، می‌توان متوجه شد که این IP متعلق به چه شخص و محلی است و به این ترتیب،

هویت شما می‌تواند آشکار شود. برای حل این مشکل، باید از یک واسطه یا «Proxy» کمک بگیرید تا به جای IP شما، IP واسطه برای مقصد آشکار شود. برای پیدا کردن واسطه مطمئن، از افراد متخصص مورد اعتماد خود کمک بگیرید یا از نرم‌افزارهایی که مورد اطمینان عمومی است، مانند Psiphon (سایفون) و Tor استفاده کنید.

به سایت‌های ایرانی فروشنده راهکارهای عبور از فیلتر اعتماد نکنید. بعضی از سایت‌هایی که راهکار عبور از فیلتر را به کاربران ایرانی می‌فروشند، تمام اطلاعات رد و بدل شما را کنترل و ثبت می‌کنند.

از HTTPS استفاده کنید. اینگونه می‌توانید اطمینان بیشتری از آدرسی که قصد بازدید از آن را دارید داشته باشید.

در مورد ای‌میل ذکر این موارد خالی از لطف نیست: ۱) از سرویس‌های ای‌میل مطمئن، بخصوص Gmail استفاده کنید. ۲) گذرواژه ای‌میل خود را فقط برای ای‌میل استفاده کنید و هرگز آن را در اختیار سایت‌های دیگر قرار ندهید. ۳) هنگامی که ای‌میلی را باز می‌کنید، روی پیوندهایی که داخل ای‌میل وجود دارد تا حد امکان کلیک نکنید. ۴) فریب کلاه‌برداری‌ها و نظرخواهی‌های ای‌میلی را نخورید. ۵) حتماً چند ای‌میل برای کارهای مختلف داشته باشید. ۶) دیدن تصاویر و دسترسی به فایل‌ها و پیوندهایی که در داخل متن ای‌میل (نه قسمت الصاق‌ها یا Attachments) است، می‌تواند IP شما را برای منابع دیگر لو بدهد. پس مراقب این پیوندها باشید.

چت کردن و استفاده از Messengerها

بسیاری از راهکارهای فیلترشکن در مورد نرم‌افزارهای چت کردن، بی‌تأثیر خواهند بود، زیرا بسیاری از راهکارهای امنیتی فقط در مورد «مرورگر وب» کارآیی دارند. پروکسی‌ها و VPNهایی که تمام ارتباطات اینترنتی شما را پوشش می‌دهند این امکان را دارند که امنیت شما را هنگام چت کردن بالا ببرند. همچنین، مراقب فایل‌هایی باشید که از طریق نرم‌افزارهای چت برای شما فرستاده می‌شود و ندانسته روی پیوندهای ارسالی، کلیک نکنید.

از اطلاعات شخصی خود محافظت کنید

هنگام وارد کردن نام کاربری و گذرواژه خود، اطمینان حاصل کنید که آدرس صفحه همان سایت مورد نظر شما است. همچنین، برخی از سایت‌ها از شما می‌خواهند تا گذرواژه ای‌میل خودتان را وارد کنید تا دوستان شما را دعوت کنند. اگر به سایت اعتماد کامل ندارید، هرگز این کار را نکنید. همچنین هنگام عضویت در سایت‌ها گذرواژه‌ای که برای سایت می‌سازید، با گذرواژه ای‌میل‌تان یکسان نباشد.

می‌توان با تحقیقات و بررسی‌هایی، رد پای شما در اینترنت و اطلاعات پراکنده‌ای را که این‌سو و آن‌سو بر جای گذاشته‌اید، به هم متصل کرد و هویت شما را شناسایی کرد. همیشه از ایمیل‌های جدید استفاده کنید و اطلاعات غیر لازم از خود را در سایت‌ها وارد نکنید.

سایت‌های اجتماعی

سایت‌های اجتماعی مانند Facebook و Google Plus و Manjam می‌توانند در صورت سهل‌انگاری شما تبدیل به یک خطر جدی امنیتی شوند. برای پیش‌گیری از چنین خطرها و نتایجی، به موارد زیر توجه کافی مبذول دارید:

- ایجاد شناسه‌های مجزا
- پرهیز از نشر اطلاعات شخصی
- توجه به ارتباطات و تماس‌های دوستانه

از شبکه‌هایی که کاربران زیاد دارند به اینترنت متصل شوید

اگر از اینترنت اداره یا دانشگاهی که کاربران کمی دارد استفاده می‌کنید، مراقب باشید چون بیشتر در معرض خطر شناسایی خواهید بود. ممکن است حتی از روی تاریخ انتشار مطالب شما بر روی اینترنت بتوان شما را شناسایی کرد.